

Implementation of Geoblocking in Palo Alto Next-Generation Firewalls using Geolocation

Avery Schiro, Andrew Clements
Advisor: Ali AlSabeH

Department of Integrated Information Technology
University of South Carolina

22 April 2022



Agenda

Introduction

Purpose

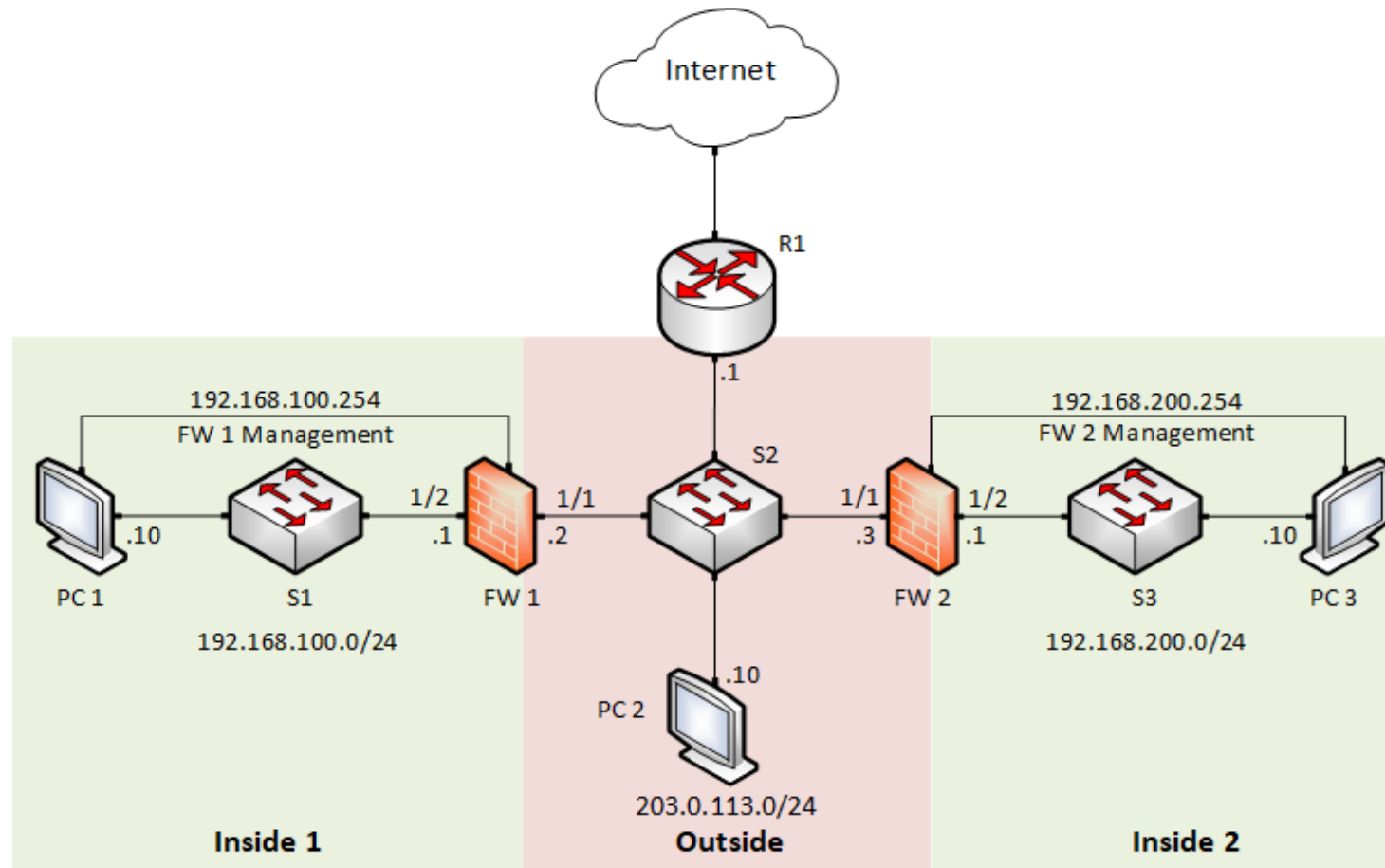
Proposed Solution

Analyzing Solution

Conclusion



Introduction



Purpose

- Understand Geoblocking
- Implement Geoblocking security policies
- Test Geoblocking security policies
- Analyze browser and router traffic on network



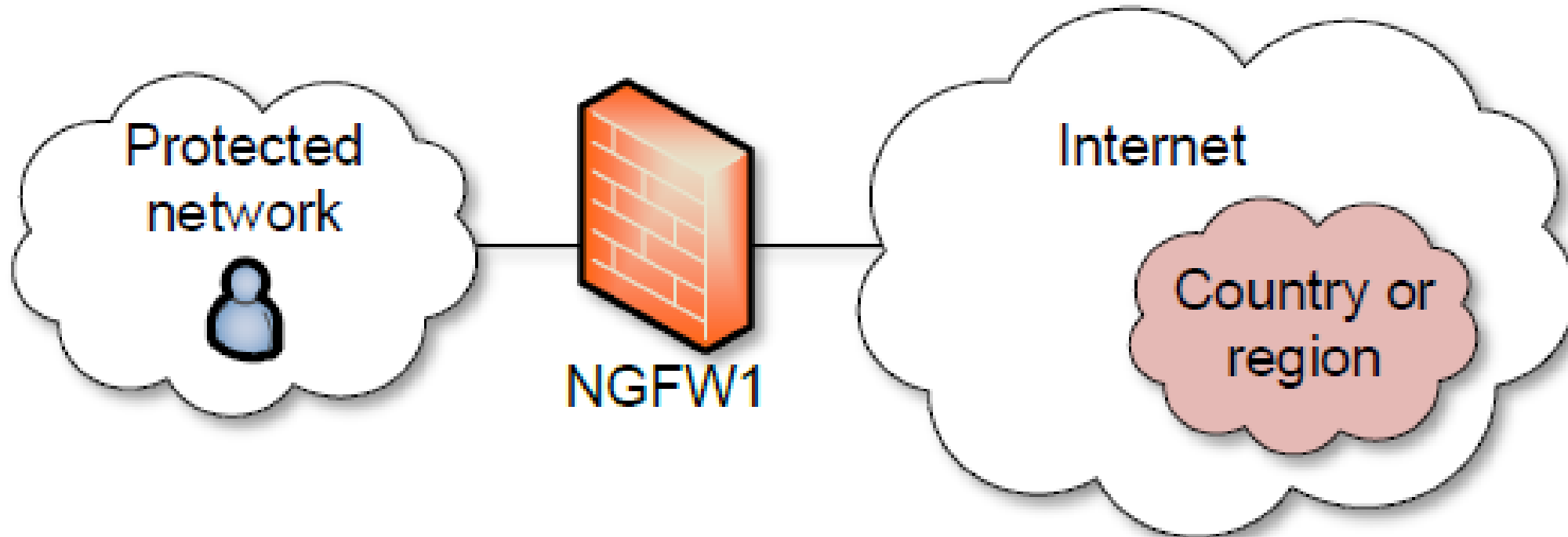
Proposed solution and implementation

Create two policies; one to restrict incoming packets and one to restrict outgoing packets from a selected location.

	Name	Tags	Type	Source		Destination		Application	Service	Action
				Zone	Address	Zone	Address			
1	incoming-block-China	none	universal	Outside	CN	Inside 2	any	any	application-default	Deny
2	outgoing-block-Ccina	none	universal	Inside 2	any	Outside	CN	any	application-default	Deny
3	any-zone-to-any-zone	none	interzone	any	any	any	any	any	any	Allow
4	intrazone-default	none	intrazone	any	any	(intrazone)	any	any	any	Allow
5	interzone-default	none	interzone	any	any	any	any	any	any	Deny



Analyzing Solution



Blocking all traffic going to and from China using those two policies.



Analyzing Solution

- Search traffic logs by the website.
 - Ability to know the web address in China.
 - Identify to rule and session end reason.







	Receive Time	Type	From Zone	To Zone	Source	Destination	To Port	Application	Action	Rule	Session End Reason	Bytes
	04/07 14:31:51	drop	Inside 2	Outside	192.168.200.10	117.136.190.162	443	not-applicable	deny	outgoing-block-China	policy-deny	74
	04/07 14:31:50	drop	Inside 2	Outside	192.168.200.10	117.136.190.162	443	not-applicable	deny	outgoing-block-China	policy-deny	74
	04/07 14:31:46	drop	Inside 2	Outside	192.168.200.10	117.136.190.162	443	not-applicable	deny	outgoing-block-China	policy-deny	74



Analyzing Solution

- Search traffic logs by PC address / Destination.
- Ability to know the destination address of ping.
- Identify to rule and session end reason.



	Receive Time	Type	From Zone	To Zone	Source	Destination	Application	Action	Rule	Session End Reason	Bytes	HTTP/2 Connection
	04/07 16:22:51	drop	Outside	Inside 1	202.130.245.42	192.168.100.10	ping	deny	incoming-block-china	policy-deny	300	0
	04/07 16:21:07	drop	Outside	Inside 1	202.130.245.42	192.168.100.10	ping	deny	incoming-block-china	policy-deny	300	0
	04/07 16:18:30	drop	Outside	Inside 1	202.130.245.42	192.168.100.10	ping	deny	incoming-block-china	policy-deny	300	0
	04/07 16:12:51	drop	Outside	Inside 1	202.130.245.42	192.168.100.10	ping	deny	incoming-block-china	policy-deny	300	0



Conclusion

- Implementation successful of 2 policies
 - Incoming traffic blocked successful
 - Outgoing traffic blocked successful
 - Verification of blocked packets with logs
- Question?
- Thank You for listening and watching
- Net Lab demonstration

